Network Manager

8.0-7-0

Release Notes

This general availability release of Network Manager introduces several new features and fixes to improve user experience and performance.

For all other Network Manager features, see the accompanying Network Manager 8.0 documentation.

IMPORTANT Take the backup of server database before upgrading the EzRF server.

In this Release...

Application Visibility

Network Manager introduces support for monitoring and blocking traffic based on applications used by clients in your network. By default, Network Manager allows all application traffic and monitoring data is shown as cumulative value of all usage.

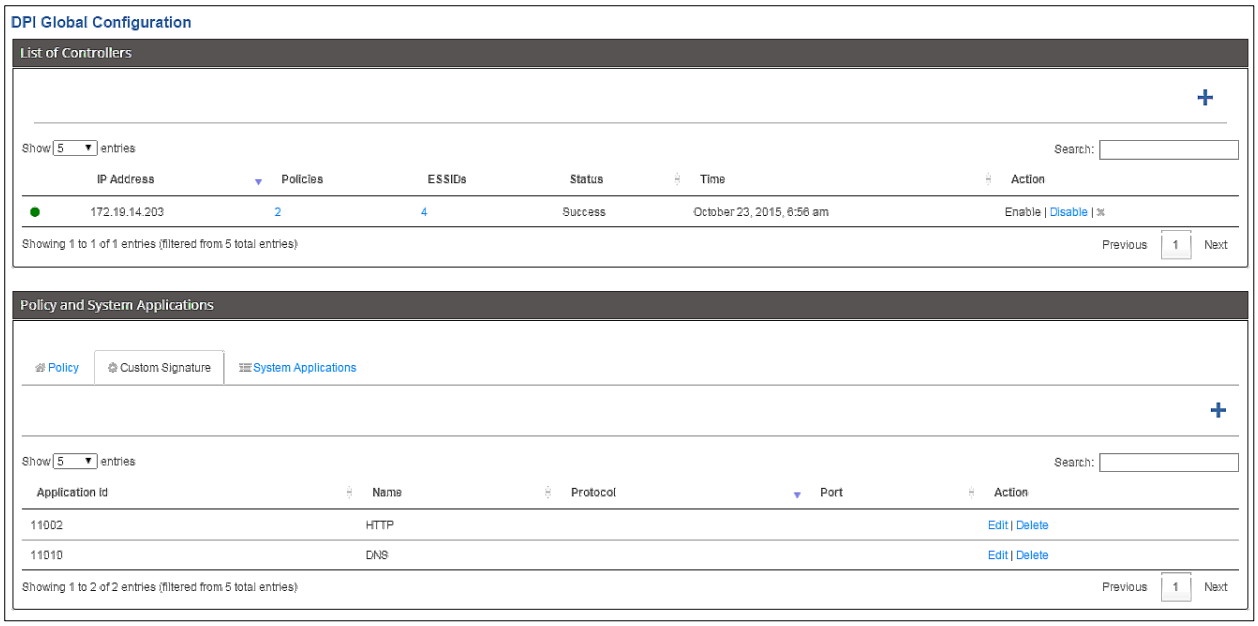
The application visibility feature in Meru Network Manager allows you to do the following:

1. Monitor application traffic
2. Block applications
3. Create and push policies to controller

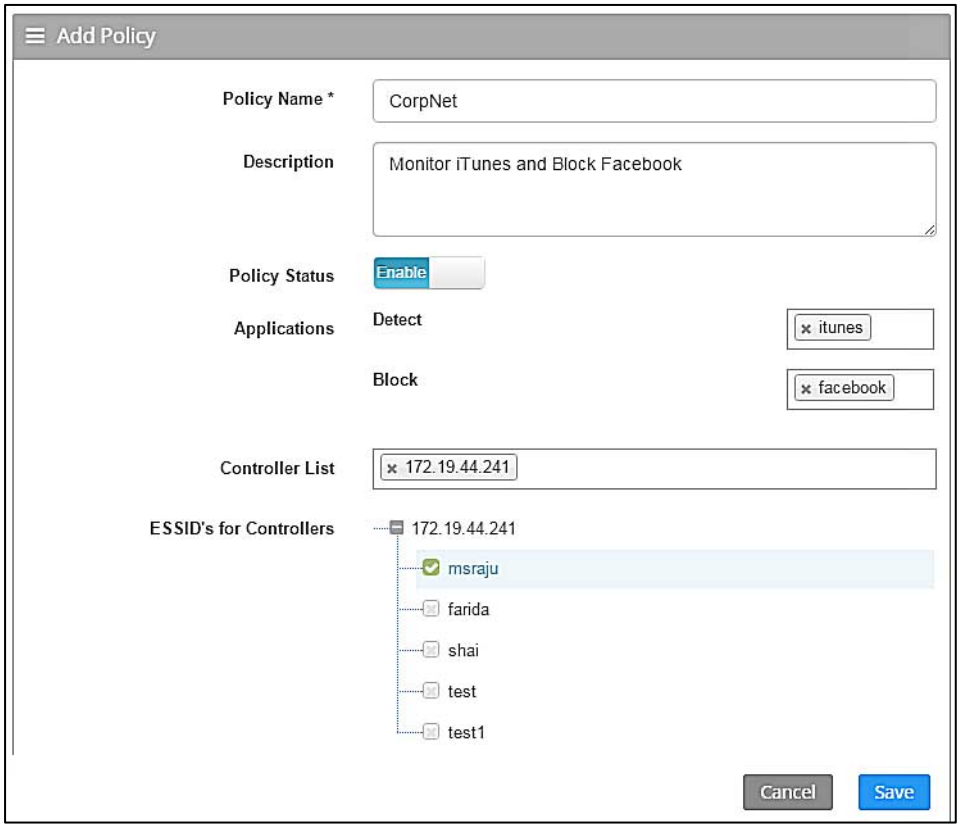
To monitor or block applications, you must create application visibility policies. Application visibility will take effect only after the policies are pushed to the controller.

To create a policy, do the following:

1. In the Network Manager WebUI, go to **Configuration** > **Application Visibility** to view the ***DPI Global Configuration*** page.



2. Policies are defined in the **Policy and System Applications** section of the page. In the **Policy** tab, Click the + icon to create policies in the **Add Policy** settings window. Enter the following details to create a policy rule:

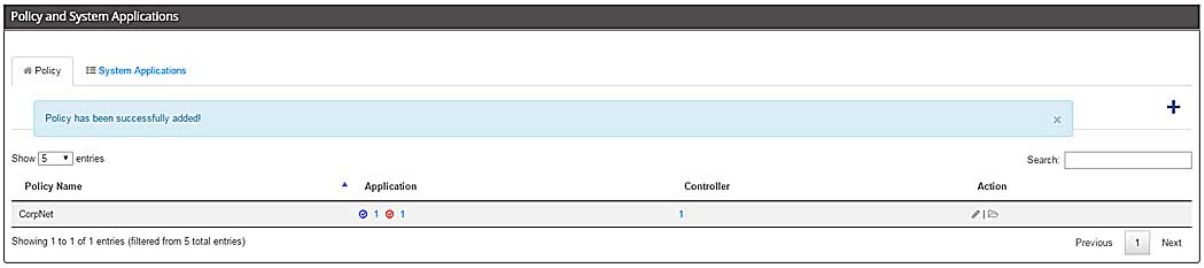


3. Specify a **Policy Name** to identify the policy
4. Provide Description for the policy.
5. Toggle the **Profile Status** switch to Enable

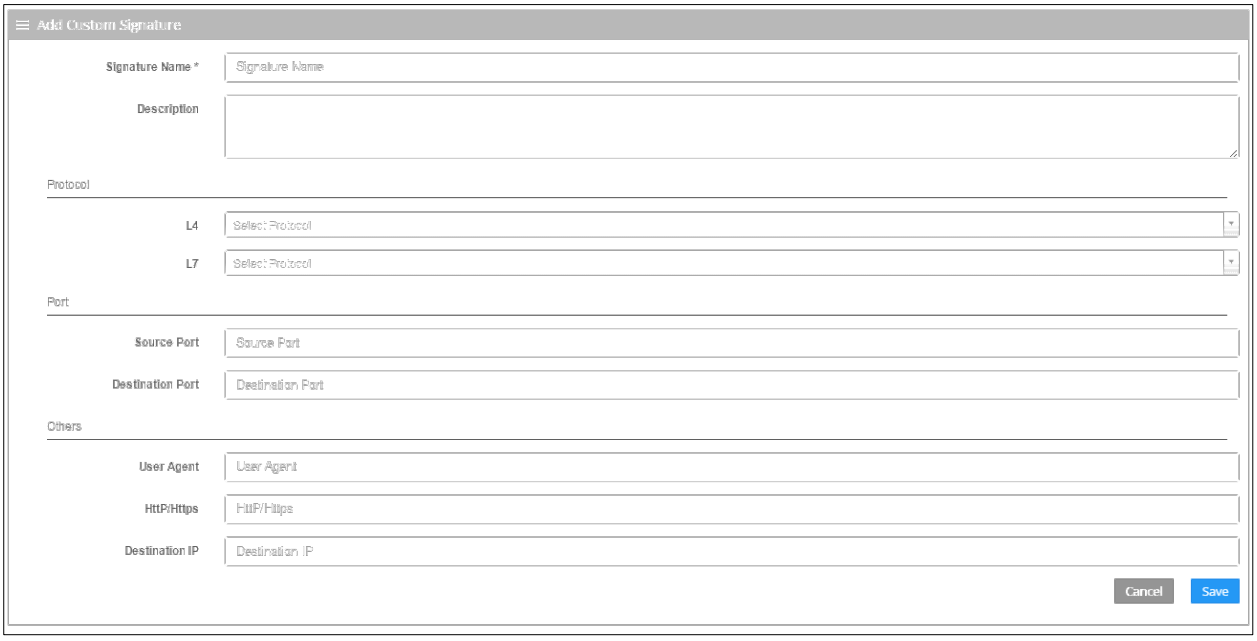
6. To add applications for monitor or to block, click either the **Detect** text box or **Block** text to view the list of supported application and select the required application. To add more than one application click on the textbox again after adding an application.
7. Select the controller to select the required **ESSID** and click **SAVE** to add the policy.

NOTES A single policy can be used to monitor and detect applications.

After the policy is added, it is listed in the Policy and System Applications section. For each policy, this section shows the number of applications being monitored (blue color) and blocked (in red color).



Adding Custom Application

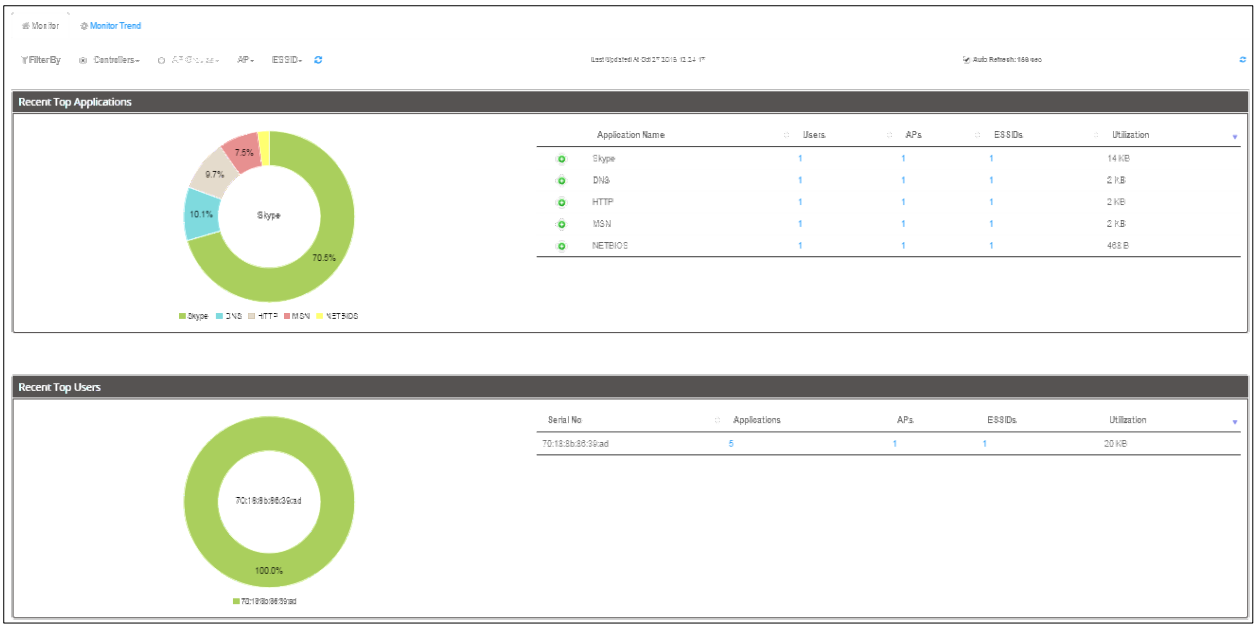


You can add custom application to a new or existing policy to monitor or block its traffic.

1. In the Network Manager WebUI, go to **Configuration** > **Application Visibility** to view the ***DPI Global Configuration*** page.
2. In the **Policy and System Applications** section of the page, go to Custom Signature tag and Click the + icon to create policies in the **Add Custom Signature** settings window

Monitoring Application Traffic

You can monitor the traffic of top 10 applications used in your network. The **Monitor** > **Global Dashboard** > **Application Visibility** dashboard provides detailed graph of top 10 applications.



The dashboard shows graphical display of traffic usage by **Applications** or Users (**Clients)**.

- **Donut chart** with top 10 applications and users. Hover over pie slices to see specific details.
    - **Tabular data** with the list of top 10 applications. For each application, you can view the following:
        - Number clients using the application
        - Number of APs serving the clients using the application
        - Number of ESSID connected to clients using the application
        - Total traffic utilization in MB.
- The **Monitor Trends** graph displays traffic usage in different intervals (2 hour, 1 day, 1 week, 1 month, and custom interval for a specified date range).
- **Data Filter** - You can filter application traffic data per Controller or AP groups. Select the **Controller** radio button and then select *AP* and *ESSID* to view application traffic for that selection.

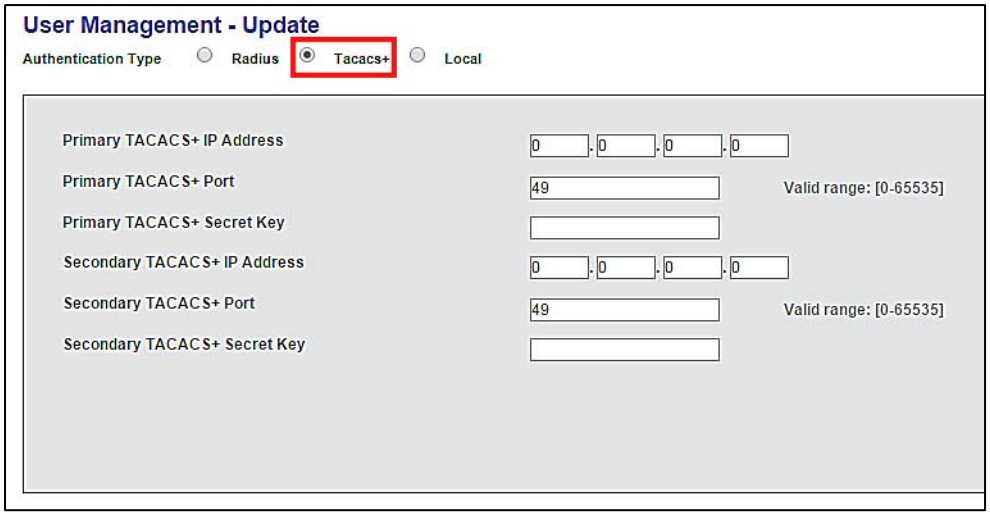
NOTE	The trend graph data is available for 2hours, 1 day, 1 week and custom timeframe using start and end date.

RADIUS and TACACS Support for Remote Administration

You can add users who can authenticate via RADIUS and TACACS server to access Network Manager servers. To add a user with TACACS login, do the following:

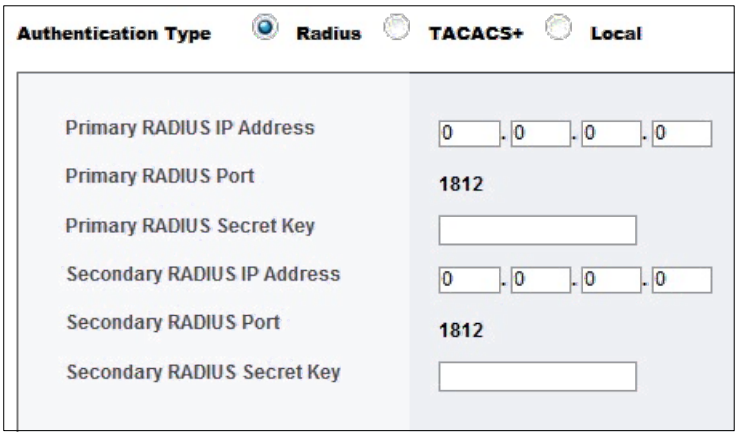
In the Network Manager WebUI, Go to **Administration** > **User Management** page.

Select the authentication type as **TACACS+** and enter the following details about the TACACS server:



Field Name	Description
Primary TACACS+ IP Address	IP address of the server
Primary TACACS+ Port	Access port of the server
Primary TACACS+ Secret Key	Password to access the server
Add secondary server details to enable redundancy.	
Secondary TACACS+ IP Address	
Secondary TACACS+ Port	
Secondary TACACS+ Secret Key	

Select the authentication type as **RADIUS** and enter the following details about the RADIUS server:



Field Name	Description
Primary RADIUS IP Address	IP address of the server
Primary RADIUS Server Port	Access port of the server
Primary RADIUS Secret Key	Password to access the server
Add secondary server details to enable redundancy.	
Secondary RADIUS IP Address	
Secondary RADIUS Port	
Secondary RADIUS Secret Key	

Captive Portal Profiles

Network Manager 8.0 introduces the captive portal profiles feature that allows you to create individual captive portal profiles with distinct configuration settings. Such captive portal profiles can be mapped to security profiles for fine control over captive portal user access.

A captive portal profile is created from the Configuration > Profiles > Captive Portal page. Profile created in this page can be applied to a security profile.

NOTE Captive Portal profile can be enabled only if at least one Captive Profile is created.

Support for 802.11w

You can now enable 802.11w support to protect WLAN management frames. Protection can be enabled for all clients or specifically for 802.11w capable clients.

Time Based ESS

You can schedule the availability of an ESS based on pre-define time intervals. By default, ESS profiles are always ON and available to clients/devices. By adding a timer, you can control the availability of an ESS profile based on pre-defined times during a day or across multiple days.

To create a time based ESS profile, you must first create a timer profile and then associate the timer profile to the ESS profile.

Creating a Timer Profile

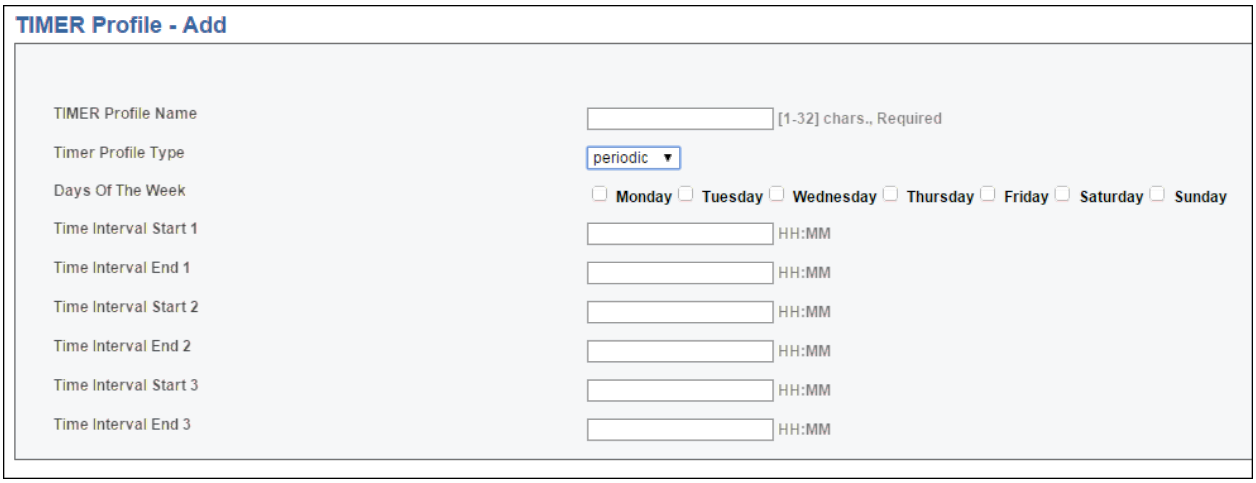
You can create timer profile using WebUI or CLI.

Using WebUI

1. Go to **Configuration** > (Profiles) **Timer** and click the **+** button.
2. In the **Add Timer Profile** window, enter *Timer Profile Name* and select *Timer Type*:

Figure 1

- **Absolute** timer profiles can enable and disable ESS visibility for time durations across multiple days. You can create up to 3 specific start and end time per timer profile. To enter start of the end time, click the Date picker box. See **label 1** in figure 1.
- **Periodic** timer profiles are a set of start and end timestamp that can be applied across multiple days of a week. To create a period timer profile, enter the time in *hh:mm* format. Where ***hh***, represent hours in 2-digits and ***mm*** represent minutes in 2-digits. Figure 2, illustrates a timer profile that will be applied on Sunday, Monday, Tuesday, and Thursday from 08:10 a.m. or 14:45 (2.45 p.m).



NOTE	Alternatively, while creating a wireless service, specify a name for the Timer profile before you click the Save button. After you click the Save button, additional tabs are opened to configure the timer-profiles.

VLAN Pooling

To reduce big broadcast or risking a chance of running out of address space, you can now enable VLAN pooling in an ESS or WPP profiles.

VLAN pooling essentially allows administrators to create a named alias using a subset of VLANs thereby creating a pool of address. By enabling VLAN pool, you can now associate a client/device to a specific VLAN. This allows you to effectively manage your network by monitoring appropriate or specific VLANs pools.

NOTE VLAN Pool is available only in tunnelled mode.

Features

- You can associate up to 16 VLANs to a pool
- You can specify the maximum number of clients that can be associated to a VLAN.
- The client/device behaviour does not change after it is associated to a VLAN in a pool.
- If a VLAN is removed from a VLAN pool, clients/devices connected to the VLAN will continue to be associated to the VLAN. However, if the clients disconnect and reconnect, their VLAN will change.

Creating a VLAN Pool

1. In the **Configuration** > (Profiles) **VLAN** page, create a VLAN.
2. Go to **Configuration** > (Profiles) **VLAN Pool** page, create a VLAN pool and specify the VLAN tag as mentioned in step 1.
3. In the **Configuration** > (Templates) **Wireless** page:
    a. Select ***Tunnel Type Interface*** as VLAN Pool
    b. Select the ***VLAN Pool Profile***.

Remote RADIUS Server

Network deployments with remote sites that are physically away from their head-quarter (or master data center –***DC***) can use remote RADIUS server in each of the remote sites for local authentication purposes.

In a typical scenario, a RADIUS server is usually co-located in the DC. Remote sites that required AAA services to authenticate their local clients use the RADIUS server in the DC. This in most cases introduces among other issues high latency between the remote site and its DC. Deploying a RADIUS server within a remote site alleviates this problem and allows remotes sites or branches to use their local AAA services (RADIUS) and not rely on the DC.

Before you Begin

Points to note before you begin deploying a remote RADIUS server:

1. Ensure that the Controller and the site AP communication time is less than RADIUS timeout.
2. Provision for at least one AP that can be configured as a relay AP.

3. Only Meru 11ac APs (AP122, AP822, AP832, and OAP832) in L3-mode can be configured as a relay AP.
4. In case of WAN survivability, no new 802.1x radius clients will be able to join, until relay AP rediscovers the controller.

How It Works

This feature provides local authentication (.1x, Captive Profile, and mac-filtering) services using a RADIUS server set up in the remote site. In addition to the RADIUS server, the remote site must also configure a Meru 11ac AP as a **relay AP.** The remote RADIUS profile can be created using Network Manager's WebUI (**Configuration** > **Profiles** > **RADIUS**). A remote RADIUS profile works like a regular profile and can be used as primary and secondary RADIUS auth and accounting servers.

IMPORTANT High latency between the remote site and DC can cause client disconnections and sluggish network experience.

About Relay AP

- The **relay AP** primarily is used for communicating between the RADIUS server (in the remote site) and the controller in the head-quarters.
- An AP is set as a relay AP only when it is assigned in the RAIDUS profile. Once an AP is assigned as a relay AP It is recommended that you do not overload the relay AP with client WLAN services. This can result in communication issues between the relay AP and DC. For regular client WLAN services, we recommend the use of a different Meru access point.
- For a remote RAIDUS profile, you cannot configure a secondary relay AP. However, for resilience purposes, we recommend configuring an alternate (backup) RADIUS profile and assigning another AP as a relay AP to this backup RAIDUS profile. In the security profile, set this RADIUS profile as the secondary RADIUS server.

The following figure illustrates a simple scenario with local RADIUS deployment

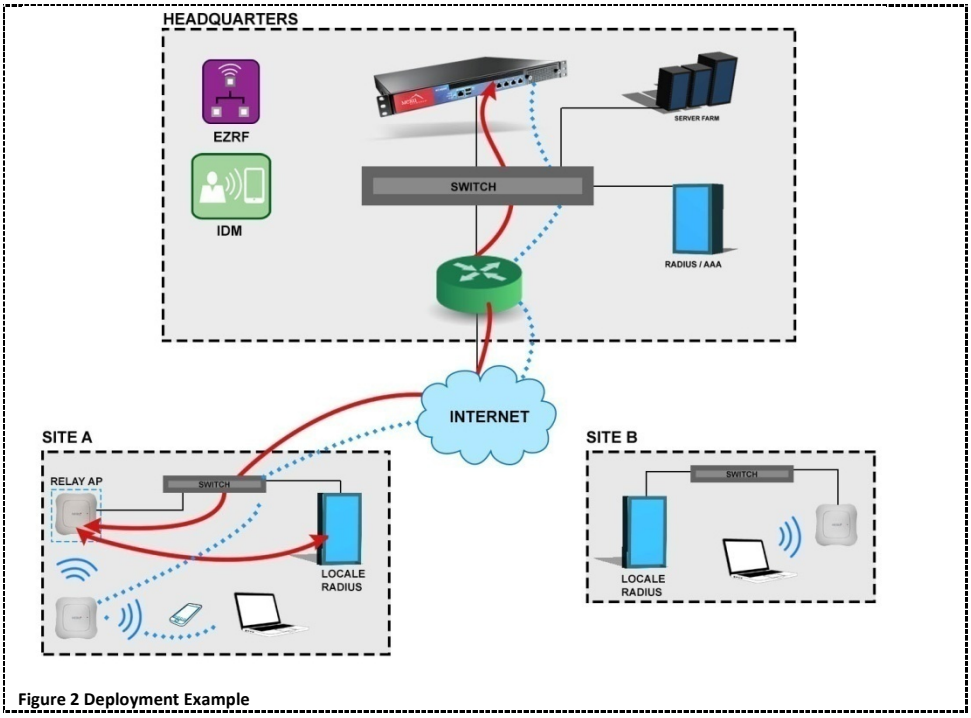
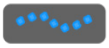


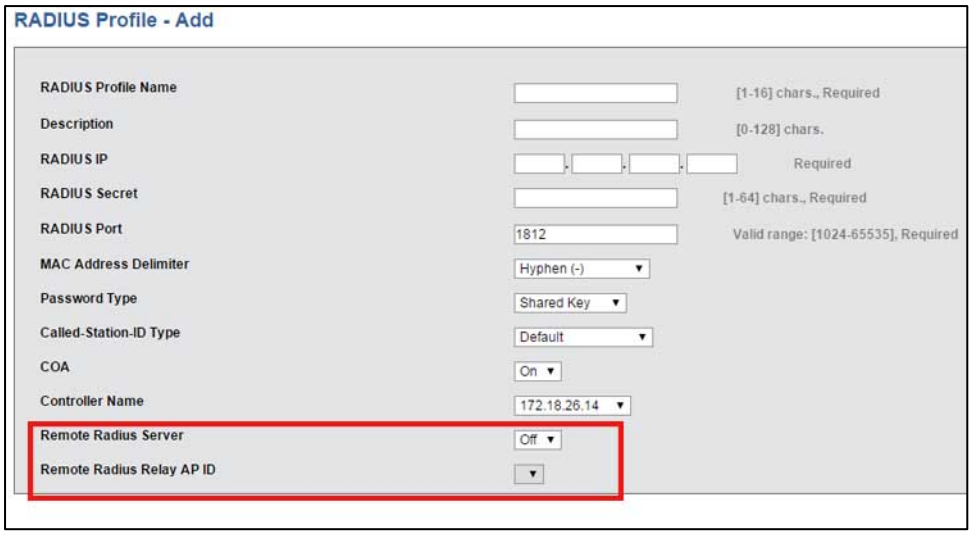
Figure 2 Deployment Example

The red line indicates the communication between the remote RADIUS server > Relay AP > Controller in headquarters.



The blue dotted line indicates regular communication (WLAN traffic) between clients, AP, and the controller in headquarters.

While creating the RADIUS profile in the Network Manager (**Configuration** > **Profiles** > **RADIUS**), enable **Remote RADIUS Server** and select a **Relay AP** (see the screenshot).



High Availability

Introducing high availability support by providing concurrent and persistent server access. HA is configured with a cluster two instances (**primary** and **backup**) of Network Manager. After setting up HA, Network Manager Server is accessed via a virtual IP. When the connection to the primary server is lost, the backup server continues to provide all services. After the primary server recovers, the control is

transferred to the primary server. New data collected by the backup server is copied and synced between both primary and backup server.

NOTE	The same license can be used in both primary and backup node. Separate licenses are not required for using High Availability

Pre-requisites

Ensure that you meet the following pre-requisites before setting HA:

- Both the instances must be running the same version of Network Manager (8.0 or above).
- Supported only on SA2000 or SA2000v models
- Both instances must be of the same model. It should be either two SA2000 or two SA2000v
- HA requires a free static IP from the same DHCP pool that provides IP address to the servers.
- Both the servers must be on the same subnet
- Backup of Master database should be restored in Backup node, before forming an HA cluster.

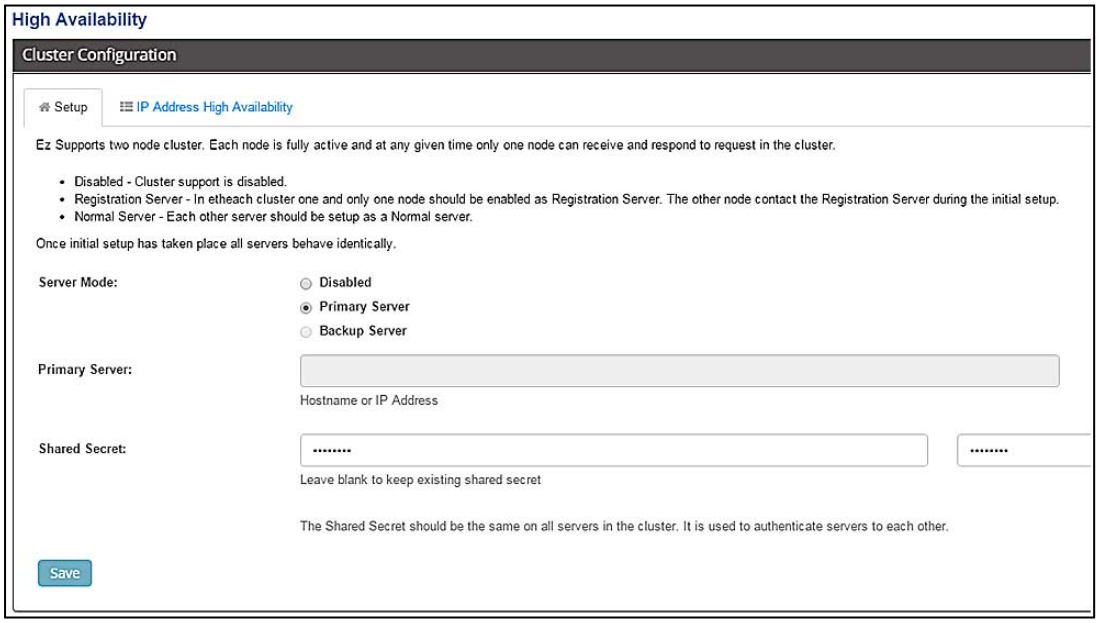
NOTE	Whenever a database restore is needed for Master or Backup nodes, cluster should be dismantled and reconfigured again after restore.

Configuring High Availability

Configuring HA requires you to add settings to both the servers (primary and backup). To begin setting up HA, access the WebUI of one of the server instance that should be configured as the primary server.

Setting up Primary Server

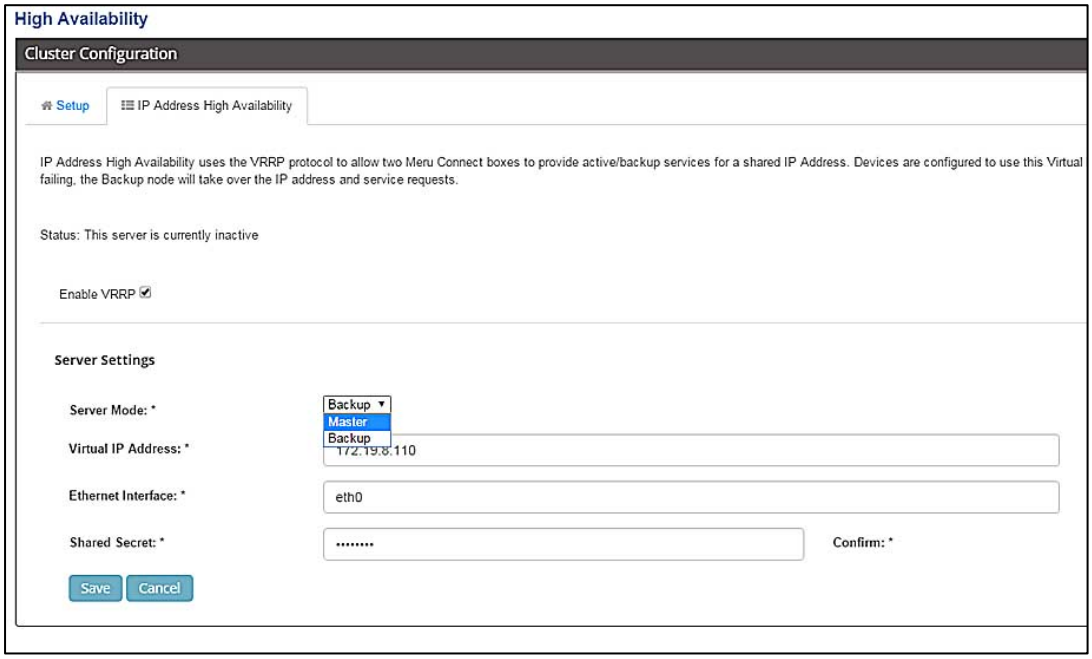
1. In the WebUI of this server, go to **Administration** > **High Availability** > **Cluster Configuration**



2. **Server Mode**: Since this server is to be configured as the primary server, select Primary Server.

3. Enter the **Secret** key.
4. Click the **Save** button to enable HA functionality.

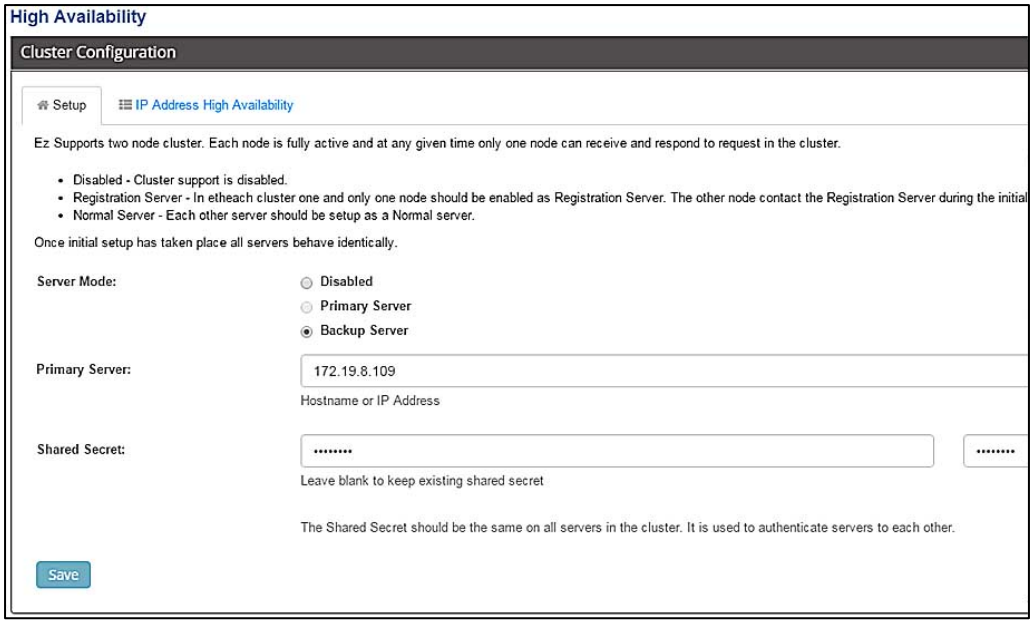
A new tab, **IP Address High Availability** is enabled only after you SAVE the primary setting. This tab provides options to configure virtual IP for HA access.



1. Enable VRRP
2. Set the **Server Mode** as ***Master***
3. Enter the **Virtual IP Address**. This address must be from the same subnet and DHCP pool use to provide the IP address of both instances of the Network Manager servers. It is recommended that you use a static IP as the virtual IP.
4. **Ethernet Interface** is automatically populated based on the model of Network Manager Servers.
5. Enter a **Shared Secret** key. This key is used by the server to maintain keep alive between the two servers.

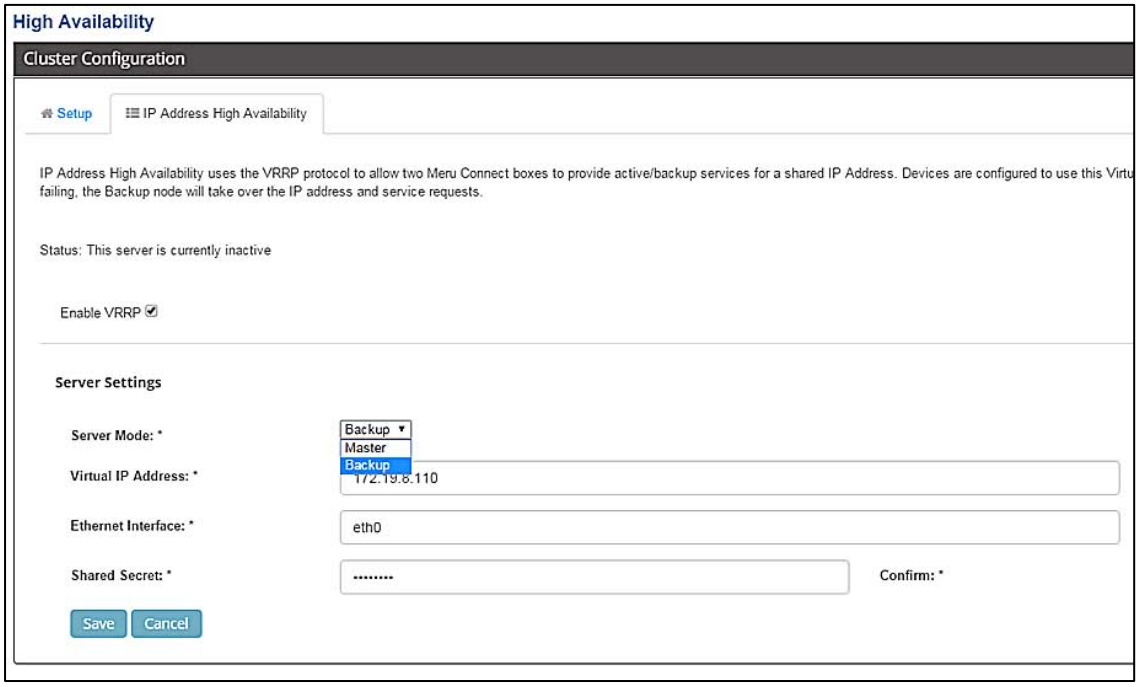
Setting up the Backup Server

In the WebUI of the second server, go to **Administration** > **High Availability** > **Cluster Configuration.**



1. **Server Mode**: Since this server is to be configured as the backup server, select Backup Server.
2. Enter the IP address of the **Primary Server**.
3. Enter the **Secret** key.
4. Click the **Save** button.

A new tab, **IP Address High Availability** is enabled only after you SAVE the primary setting. This tab provides options to configure virtual IP for HA access.



1. Enable VRRP
2. Set the **Server Mode** as ***Backup***

3. Enter the **Virtual IP Address**. This address must be from the same subnet and DHCP pool use to provide the IP address of both instances of the Network Manager servers. It is recommended that you use a static IP as the virtual IP.
4. **Ethernet Interface** is automatically populated based on the model of Network Manager Servers.
5. Enter a Shared Secret key. This key is used by the server to maintain keep alive between the two servers.

Status

Replication Status shows the available servers in the cluster. The cluster table contains status of the servers whether they are presently up or not and also shows the configured status of the server.

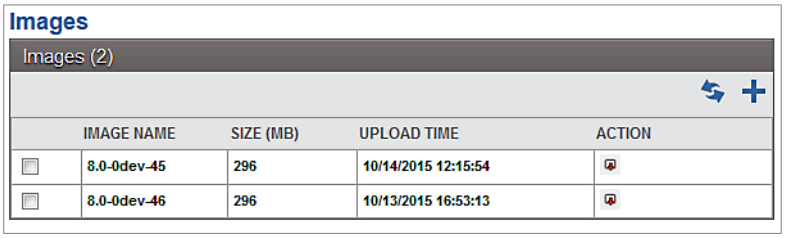
If one server is down it shows the status as "Not working". The configured server could be either Backup Server or Primary Server. User can identify the server status by logging into the server and checking the server status and for the logged in server it shows as "this server". Also users can check the configured IP addresses of the both Master and Backup node.

Software and Patch Upgrade Using WebUI

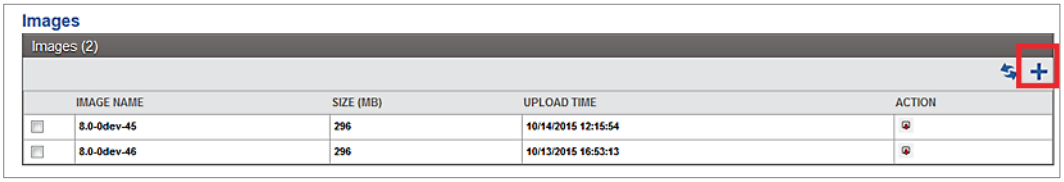
Starting with Network Manager 8.0, you can easily perform full or patch upgrade of your network manager server from WebUI.

The following procedure will guide you through the steps to upgrade your server.

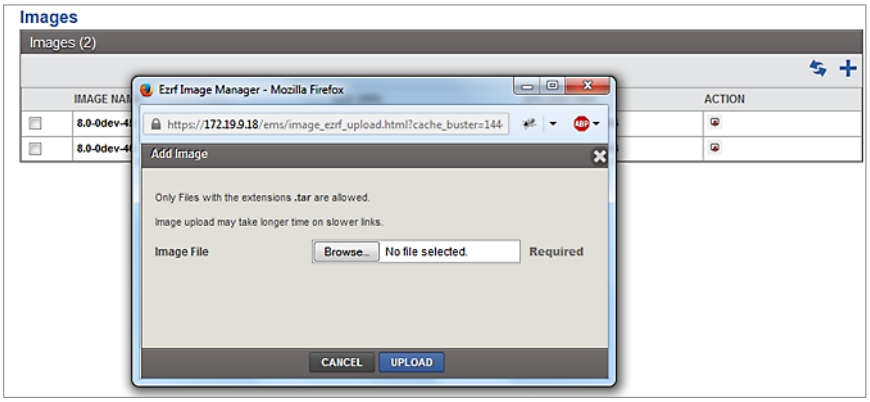
1. In the Network Manager WebUI, go to **Administration** > **Upgrade NM**. By default, this page lists all the images copied to the server.



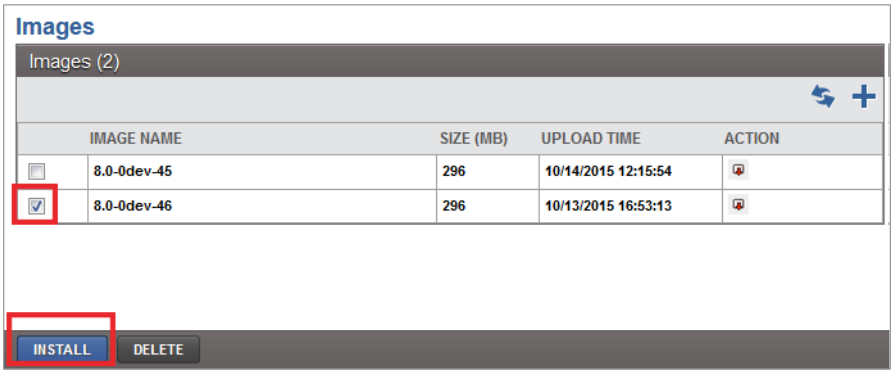
2. To upgrade your server click the **+** icon. This will open a file selector window.



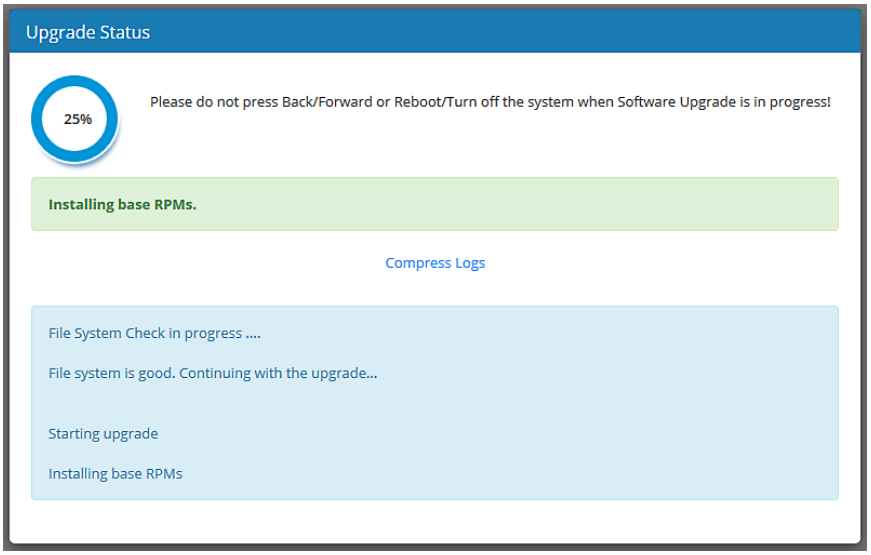
3. Select the image file from your computer or a network folder and click the **UPLOAD** button.



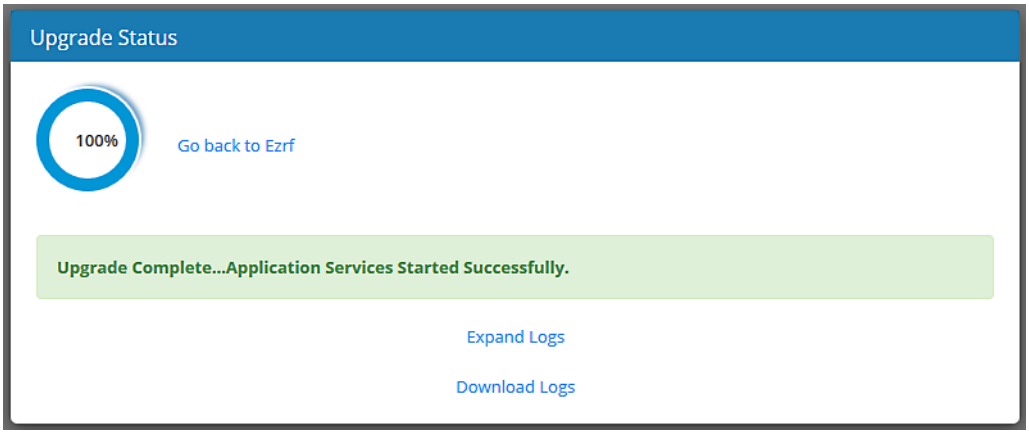
4. After the upload is complete, select the version checkbox and click the **INSTALL** button. This will begin the upgrade process.



5. During the upgrade process, do not click refresh or perform any operations on the server.



6. After the upgrade is complete, click **Go back to EzRF** link to return back to server operations.



NOTE	• In case of full upgrade, the server will restart after the upgrade process and return the page to server login prompt. • In case of patch upgrade, the server will restart the process and return to the dashboard.

List of Fixed Issues

Bug ID	Description	Scenario
48676	Deleting service profiles now correctly deletes VLAN, ESS, and security profiles.	There was an issue where deleting a service profile did not delete VLAN, ESS, and security profiles.
49782	Fixed search option issues in Custom Signature and System Applications under Policy and Sytem Applications.	NA
49407	Fixed issues that resulted in users without access to controller were able to access application visibility dashboard.	NA
49723	Fixed custom signature deletion issues from the EzRF server.	NA
49727	Fixed issues where ESS profile pushed via EzRF were missing on some of the AP's.	NA

List of Known Issues

Bug ID	Description	Scenario	Workaround
49569	Existing VPN controllers are not getting rediscovered via virtual IP in a HA cluster set up.	NA	NA

Bug ID	Description	Scenario	Workaround
49804	Certificates do not sync between master and backup node in a HA set up	NA	NA

Supported System Director Releases

Network Manager Version	Supports Controllers with these System Director Versions
8.0-7-0	• 5.3 • 6.1-2-29 • 6.1-3-6 • 7.0-x • 8.0-5-0

Supported Hardware and Software

Hardware / Software	Supported Versions/Models
Network Manager/Service Assurance Manager - Access Points	• AP110 • AP122 • AP320 • AP332 • AP433 • OAP433 • AP822 • AP832 • AP1010 • AP1020 • AP1014 • OAP832 • PSM3X
Spectrum Manager – Access Points	• AP332 • AP832 • PSM3x
Controllers	• MC1500 • MC1550 • MC3200 • MC3200-VE • MC4200 • MC4200-VE • MC5000 • MC6000
Service Appliance	• SA250 • SA2000 • SA2000-VE
Supported Browsers	• Internet Explorer 9 and later version • Mozilla Firefox 32.0 • Google Chrome, version 34.0.1847.118 m

Installing and Upgrading

This section describes procedures for upgrading your Services Appliance.

Pre-requisites for upgrade

- Ensure you have the Network Manager upgrade image for your platform. If any add-on applications are used, be sure to download the updated versions of application images. Install the image, after the Network Manager is upgraded. The following add-on applications are supported.
    - WIPS - 1.3-2-0
- Upgrade service appliance before you initiate controller (System Director) upgrade.
- While upgrading a Services Appliance with over 100 controllers, the controllers return to Active state sequentially, one at a time. It may take up to 10 minutes for all controllers to become active.

Supported Network Manager Upgrades

The following upgrade path is recommended:

- 4.0-9-0 > 6.1-2-28
- 6.1-0-9 > 6.1-2-28
- 6.1-1-5 > 6.1-2-28
- 6.1-2-28 > 6.1-3-6
- 6.1-2-28 > 7.0-5-0
- 6.1-3-6 > 7.0-5-0
- 6.1-2-8 and/or 6.1-3-6 > 8.0-7-0
- 7.0-5-0 > 8.0-7-0

NOTES	In order to upgrade the Network Manager version from 2.x to 3.1 and higher versions, the Network Manager 2.x should first be upgraded to Network Manager 3.0 and then to Network Manager 3.1 and higher versions.

Upgrade Procedure

This procedure assumes that your Services Appliance is already installed on a network.

NOTES	During the upgrade process, the DB is reset. It is therefore recommended that database backup should be taken before upgrade and restored after upgrade.

To upgrade a Services Appliance, perform the following steps:

1. Perform a complete Network Manager backup and copy the backup file to an external location. Use this if you run into a problem (Instructions for backing up the file can be found in the Maintenance chapter of the Network Manager User Guide.)
2. If you have SAM installed, disable all scheduled tests by performing the following steps:
    a. Select **Service Assurance**.
    b. From the left panel, select **Configure** > **Tests** > **Scheduled Tests**.
    c. Select the **Disable All** option and click **OK** continue.
3. Access the Services Appliance through SSH, using the administrative privilege.
4. If your appliance flash already contains three images, remove one of the older images using the `delete flash: <version number>` command.
5. Copy the file from the SCP server to your service appliance using the copy command:

    ```
    sa# copy scp://user:password@server/path/meru-nm-<releaseVersion>-SA250-rpm.tar<space>.
    ```

6. Confirm the successful transfer of the image by displaying the current flash images using the `sh flash` command:

    ```
    sa# sh flash
    6.1-3-6
    8.0-7-0
    ```

7. Upgrade the service appliance:

    ```
    sa# upgrade meru-nm-<releaseVersion>-SA250-rpm.tar
    ```

    This process installs new binaries and upgrades the stored data to the latest version. This process may take a few minutes and at the end of the upgrade the services appliance restarts. The time taken to upgrade, depends on the size of the data available on the services appliance.

8. Type the following command to confirm, if the installed software version is 8.0 BETA.

    ```
    service appliance# sh nms
    ```

    If the upgrade displays the "image integrity error," the service appliance image has been corrupted while uploading to Network Manager. Upload the new image again to the Network Manager service appliance and retry the upgrade. You can ignore the Security warning "Installing an unsigned upgrade package!" displayed by the upgrade command.

Post Upgrade Tasks

The following are optional post upgrade tasks:

1. If you have not configured for automatic transfer of backup to a remote server, then follow the instructions for configuration in the **Administration** > **Maintenance** page.
2. If required, upload the license.
3. Install the application images downloaded in the pre-requisites for upgrade section using **`upgrade feature`** command.

Downgrade

To downgrade from Network Manager to previous release, you need the previous release backup that you created when you upgraded (see step 1 of Upgrade Procedure). To downgrade to previous version, follow these steps:

1. If your appliance flash already contains three images, access the Services Appliance through SSH, logging in as admin and then remove one of the older images with the **`delete flash: <version number>`** command.
2. Downgrade the appliance to the previous release with the upgrade command:

   ```
   sa# upgrade nms-server <version number>
   ```

3. Copy the previous release backup file from the external location to the service appliance with the command copy.
4. Restore the database with the command restore.
5. While downgrading the server, error messages are displayed for missing schema file. These error messages can be ignored.
6. This completes the downgrade procedure.

Additional Resources

In addition to the release notes, the following documentation is available.

- Network Manager User Guide
- Services Appliance Installation Guide

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Support and Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service